

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 7月19日

出 願 番 号

Application Number:

平成11年特許願第205346号

出 願 人

Applicant (s):

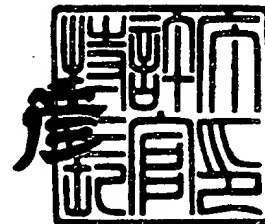
インターナショナル・ビジネス・マシーンズ・コーポレイション

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年11月19日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特平11-308150

【書類名】 特許願

【整理番号】 JA999035

【提出日】 平成11年 7月19日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 大和事業所内

【氏名】 堀越 秀人

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 大和事業所内

【氏名】 山崎 充弘

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 大和事業所内

【氏名】 田中 順

【特許出願人】

【識別番号】 390009531

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【復代理人】

【識別番号】 100079049
【弁理士】
【氏名又は名称】 中島 淳
【電話番号】 03-3357-5171

【選任した復代理人】

【識別番号】 100084995
【弁理士】
【氏名又は名称】 加藤 和詳
【電話番号】 03-3357-5171

【選任した復代理人】

【識別番号】 100085279
【弁理士】
【氏名又は名称】 西元 勝一
【電話番号】 03-3357-5171

【選任した復代理人】

【識別番号】 100099025
【弁理士】
【氏名又は名称】 福田 浩志
【電話番号】 03-3357-5171

【手数料の表示】

【予納台帳番号】 006839
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9304391
【包括委任状番号】 9304392

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ機能付きコンピュータおよび方法

【特許請求の範囲】

【請求項1】 コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

(a) 前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第1の記憶手段に記憶し保持するステップと、

(b) 前記ステップ(a)のあとに前記コンピュータのパワー・オン中または省エネ・モード中に前記コンピュータに前記セキュリティ装置が装着されていることを検出するステップと、

(c) 前記ステップ(b)の検出結果を示す装着データを前記コンピュータに装備された第2の記憶手段に記憶し保持するステップと、

(d) 前記設定データ及び前記装着データに基づいて前記コンピュータから前記セキュリティ装置が脱着されたことを検出するステップと、

(e) 前記ステップ(d)の検出結果に基づいて前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項2】 前記ステップ(e)は所定のパスワードの入力により回避可能であることを特徴とする請求項1に記載の方法。

【請求項3】 コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

(a) 前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第1の記憶手段に記憶し保持するステップと、

(b) 前記ステップ(a)のあとに前記設定データに基づいて前記コンピュータに装備された内蔵基本電源線の連結手段を連結し電力供給線を確保するステップと、

(c) 前記コンピュータに前記セキュリティ装置が装着されて前記内蔵基本電

源の電力供給路を形成しているときに前記連結手段の連結を遮断するステップと

(d) 前記ステップ(c)における前記連結の遮断を維持するステップと、

(e) 前記連結の遮断により前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項4】 前記ステップ(d)は、前記コンピュータの前記内蔵基本電源の電力供給により維持することを特徴とする請求項3記載の方法。

【請求項5】 セキュリティ装置の装着ができるコンピュータであって、前記コンピュータの主電源が停止している状態で記憶保持が可能な第1の記憶手段と、

前記コンピュータの主電源が停止しかつ副電源が作動している状態で記憶保持が可能な第2の記憶手段と、

演算処理装置と、

a) 前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第1の記憶手段に記憶し保持するステップと、(b) 前記ステップ(a)のあとに前記コンピュータのパワー・オン中または省エネ・モード中に前記コンピュータに前記セキュリティ装置が装着されていることを検出するステップと、(c) 前記ステップ(b)の検出結果を示す装着データを前記コンピュータに装備された第2の記憶手段に記憶し保持するステップと、(d) 前記設定データ及び前記装着データに基づいて前記コンピュータから前記セキュリティ装置が脱着されたことを検出するステップと、(e) 前記ステップ(d)の検出結果に基づいて前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第3の記憶手段と

を有するコンピュータ。

【請求項6】 セキュリティ装置の装着ができるコンピュータであって、前記コンピュータの主電源が停止している状態で記憶保持が可能な第1の記憶手段と、

内蔵基本電源により作動し内蔵基本電源線を連結する連結手段と、
演算処理装置と、

(a) 前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第 1 の記憶手段に記憶し保持するステップと、(b) 前記ステップ (a) のあとに前記設定データに基づいて前記コンピュータに装備された内蔵基本電源線の連結手段を連結し電力供給線を確認するステップと、(c) 前記コンピュータに前記セキュリティ装置が装着されて前記内蔵基本電源の電力供給路を形成しているときに前記連結手段の連結を遮断するステップと、(d) 前記ステップ (c) における前記連結の遮断を維持するステップと、(e) 前記連結の遮断により前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第 2 の記憶手段と

を有するコンピュータ。

【請求項 7】 前記第 1 の記憶手段が R F I D システムに使用する R F I D タグであり、前記セキュリティ装置が R F アンテナ及び第 1 接続手段である請求項 5 または 6 に記載のコンピュータ。

【請求項 8】 前記 R F アンテナ及び第 1 接続手段が前記コンピュータのデバイス・ベイの蓋に装着されている請求項 5 乃至請求項 7 のいずれかに記載のコンピュータ。

【請求項 9】 前記連結手段がアナログスイッチである請求項 6 乃至請求項 8 のいずれかに記載のコンピュータ。

【請求項 1 0】 前記セキュリティ装置が R F アンテナ、第 1 接続手段及び第 2 接続手段である請求項 9 に記載のコンピュータ。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンピュータの盗難および不正アクセス等を防止するためにコンピュータ本体に取り外し可能に装着されたセキュリティ機能の一部を担う装置が取り外された場合に、コンピュータへのアクセスを禁止する技術に関する。

【0002】

【従来の技術】

ノートブック型コンピュータは携帯性に優れている反面、きわめて容易に不正に外部に持ち出される。近年のコンピュータ利用の高度化および多様化に伴い、ユーザは貴重な情報をコンピュータ内部に格納する傾向がますます強まり、コンピュータが盗難に合うとその物理資源の損失に比べて情報資源の漏洩による損失が一層甚大になってきている。

【0003】

特開平8-50690号公報および特開平10-124764号公報は、RF（ラジオ周波数）トランスポンダ・システムという非接触的な通信技術を用いた電子式物品監視システムを開示する。RFトランスポンダ・システムは、一般的に励振器（E x i c i t e r）／読取器（R e a d e r）すなわちER、およびRFIDトランスポンダあるいはRFID（Radio Frequency Identification）タグと呼ばれるものを含んでいる。監視区域内の物品にRFIDタグを取り付け、その領域の出入口にERを設置して常時RF励振信号を発生させる。出入口にRFIDタグが取り付けられた物品が接近するとERがこれに励振信号を送信して電力を与えるのでRFIDタグ自体は特に動作の電力を必要としない。RF励振信号を受け取ったRFIDタグは識別コードその他のデータ信号を発生し、特定の周波数でERに応答信号として送り返す。この応答信号中に含まれる識別コードをERが検出すると必要に応じてアラーム音を発生して物品の盗難を防止する。物品を監視区域内からアラーム音を発生させないで持ち出すには、RFIDタグをアラーム信号を送信しない状態にセットするかこれを脱着する必要がある。

【0004】

特開平5-35354号公報は、ノートブック型コンピュータの盗難防止を図る技術を開示する。ノートブック型コンピュータに、設置傾斜量、設置圧力および設置距離等の設置状態の変化を検出する盗難防止手段と設置状態の変化に応答して警報を発する手段を設ける。これらの手段が機能を発揮する状態にあるときコンピュータは設置状態を常時監視し、コンピュータを許可なく定位置から持ち

運ぼうとした際に警報を発して盗難を防止する。

【0005】

特開平3-100894号公報は、携帯端末が盗難に合ったときにキー入力を停止して不正なアクセスを禁止する技術を開示する。携帯端末が盗難に合うと、ホストコンピュータから無線で端末に特定の信号を送り、それに応答して端末内部のプログラムが作動してキー入力ができない状態にする。

【0006】

【発明が解決しようとする課題】

上述したようにRFIDタグを使用して物品の盗難を防止する技術が知られており、またノートブック型コンピュータが監視区域から不正に持ち出されることを防止する技術およびコンピュータの盗難時にキー入力をロックして情報資源を保護する技術も知られている。しかし、RFIDタグをコンピュータに装着して盗難に合ったコンピュータへの不正アクセスを防止する技術は開示されていない。

【0007】

ところで、盗難防止または記憶情報への不正アクセスを防止するには、コンピュータにRFIDタグのような装置を装備する必要がある。一方このような装置は、すべてのユーザが必要とするものではなく、一般に企業内で大規模に使用している場合に比べて個人的範囲でのみ使用するユーザにとっては必要性が少ない。セキュリティ機能をすべてのコンピュータに装備して販売することは、必要のないユーザに対して余分な費用を強いることになり好ましくない。したがって、特定のシリーズに含まれる同一タイプのコンピュータにおいて、セキュリティ機能を装備するものとセキュリティ機能を装備しないものとを用意する必要がある。

【0008】

ところで、特定のシリーズに含まれるコンピュータは、できるだけハードウェアおよびソフトウェアの共通化を図ることが販売コストおよび販売後のサービスの維持という面で好ましい。特定のシリーズのコンピュータをセキュリティ機能を装備するものと装備しないものとに分けて製造および販売することは、一見セ

セキュリティ機能を必要としないユーザの費用負担を公平にできるようにみえるが、共通化ができない部分での費用負担が増加し結果としてそのようなユーザにとっても不利になる。ここに、ハードウェアおよびソフトウェアの共通化とユーザによるセキュリティ機能の選択による費用負担の公平性という課題を同時に解決する必要が生じてくる。

【0009】

これを解決する方法として、あるセキュリティ機能が複数のハードウェアおよびソフトウェアの構成要素からなる場合にその構成要素のある部分までを共通にし、残りの一部を販売店またはユーザが必要に応じて追加できるオプション部品にしてセキュリティ機能を完成できるようにする方法がある。しかし、セキュリティ機能の一部を担う装置をユーザまたは販売店で装着するようにすると（このような装置を以後単にセキュリティ装置という。）、その部分が不正に脱着されてセキュリティ機能が毀損されてしまうことが予測される。

【0010】

したがって本発明の目的は、コンピュータのセキュリティ機能を担う一部の装置、すなわちセキュリティ装置がコンピュータから脱着されたときに、コンピュータへのアクセスを禁止する技術を提供することにある。また、本発明の他の目的は、ユーザまたは販売店がオプションに取り付けるセキュリティ装置の好適な取り付け構造を提供することにある。

【0011】

【課題を解決するための手段】

本発明に係るコンピュータはセキュリティ装置をオプションに取り付けることができる構造を備え、セキュリティ装置を装着することによりセキュリティ機能を具備したコンピュータを構成し、セキュリティ装置を脱着することでセキュリティ機能を具備しないコンピュータを構成する。本発明においてコンピュータへのアクセスを禁止する手順は、コンピュータのパワー・オン、省エネ・モード、特に最小エネルギー・モード等の特定のイベントに関連付けて開始させることができるが、常時CPUにポーリングにより監視させてもよい。特定のイベントに関連付けて開始させると、CPUの負担を軽くすることができる。

【0012】

本発明の第1の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、(a) 前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第1の記憶手段に記憶し保持するステップと、(b) 前記ステップ(a)のあとに前記コンピュータのパワー・オン中または省エネ・モード中に前記コンピュータに前記セキュリティ装置が装着されていることを検出するステップと、(c) 前記ステップ(b)の検出結果を示す装着データを前記コンピュータに装備された第2の記憶手段に記憶し保持するステップと、(d) 前記設定データ及び前記装着データに基づいて前記コンピュータから前記セキュリティ装置が脱着されたことを検出するステップと、(e) 前記ステップ(d)の検出結果に基づいて前記コンピュータへのアクセスを禁止するステップとを備える。

【0013】

本発明においてセキュリティ装置とは、コンピュータのセキュリティ機能の一部を担うハードウェアであって、オプション部品として用意されユーザまたは販売店で脱着可能な程度の装着容易性を備える装置をいう。例えばRFIDを利用したセキュリティ・システムではRFアンテナでもよく、指紋検出を利用したセキュリティ・システムでは指紋入力部であってもよい。さらにセキュリティシステムではジャンパ等の接続部材を含んでいる。第1の記憶手段はコンピュータの主電源が停止した状態で記憶内容を保持できる記憶媒体でEEPROMまたはハードディスク等を選定できる。さらに2次電池により主電源が停止している場合でも記憶保持ができる電力が供給され続けているRAMであってもよい。また、第2の記憶手段は主電源が停止しかつ副電源(電池や省エネ・モードによる電源)が作動している場合に記憶保持ができ電力が供給され続けているRAMや回路素子等を選定できる。また、コンピュータには電池等の内蔵基本電源が備えられており、この内蔵基本電源ではコンピュータの構成情報等の基本的な構成情報をバックアップするためのCMOSメモリに電力供給される。この手順はセキュリティ機能を備えるコンピュータおよび備えないコンピュータのいずれに対して

も共通に実行でき、セキュリティ機能を備えるコンピュータについてのみセキュリティ装置が脱着されたときにアクセスが禁止される。

【0014】

上記第1の態様においては、ステップ(a)により、このコンピュータがセキュリティ機能を備えるべく設定した設定データが記憶される。この設定データは、セキュリティ装置の装着前に設定してもよいし、装着後に設定してもよい。このコンピュータがセキュリティ機能を備えたコンピュータであることがシステムにより認識され、コンピュータからセキュリティ装置が脱着された場合は不正行為があったものとして以下の手順によりパスワードを入力しない限りコンピュータへのアクセスが禁止される。ステップ(b)により、このコンピュータがセキュリティ機能を備えるコンピュータであることが確認される。この確認は、セキュリティ装置に導通部位を有させ、この導通部位が存在することを検知することによって可能となる。そして、ステップ(c)によりコンピュータに対するセキュリティ装置の装着または脱着の状態が保持される。保持はメモリのみならずフラグ設定やカウンタ等の計数によっても可能である。次に、ステップ(d)により、セキュリティ装置の脱着が確認され、セキュリティ装置が装着状態から脱着したとき、これは不正行為としてステップ(e)でコンピュータへのアクセスが禁止される。適正にセキュリティ装置を脱着する場合は、パスワードを入れてアクセスを確保することができる。

【0015】

本発明の第2の態様は、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、(a)前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第1の記憶手段に記憶し保持するステップと、(b)前記ステップ(a)のあとに前記設定データに基づいて前記コンピュータに装備された内蔵基本電源線の連結手段を連結し電力供給線を確認するステップと、(c)前記コンピュータに前記セキュリティ装置が装着されて前記内蔵基本電源の電力供給路を形成しているときに前記連結手段の連結を遮断するステップと、(d)前記ステップ(c)における前記連結の遮断を維持するステップと、(e)

）前記連結の遮断により前記コンピュータへのアクセスを禁止するステップとを備える。

【 0 0 1 6 】

上記第 2 の態様では、ステップ (b) においてリチウムバッテリー等の連結すなわち内蔵基本電源の電力線を導通させる。この導通は、アナログスイッチ等の連結手段により可能である。これにより、セキュリティ機能を備えていないコンピュータであっても内蔵基本電源が遮断されることがない。ステップ (c) では、一旦セキュリティ装置が装着されてこのコンピュータがセキュリティ機能を備えるコンピュータであることをシステムが認識したのちでセキュリティ装置により内蔵基本電源の電力供給路が形成されているときに連結を遮断する。これは、セキュリティ装置により内蔵基本電源の電力供給路が形成されているため、連結を解除しても内蔵基本電源が遮断されることがないためである。ステップ (d) では、連結の遮断を維持している。この連結の遮断は初期化の困難性が必要があるため、内蔵基本電源の電力供給によりなされることが好ましい。セキュリティ装置が取り外された場合、そのコンピュータに対して不正なアクセスであるときは内蔵基本電源の電力供給路が絶たれ内蔵基本電源から電力供給されていたコンピュータ内部のものが初期化されるので、ステップ (e) によりコンピュータへのアクセスが禁止される。

【 0 0 1 7 】

本発明の第 1 の態様及び第 2 の態様で説明した各ステップは、コンピュータ・プログラムによりコンピュータ上で実行させることができる。このようなプログラムは第 3 の記憶手段として利用できる E E P R O M または F L A S H R O M といわれる不揮発性のメモリや、ハードディスク、フロッピー・ディスク等に記憶させることができ、コンピュータの動作時にメイン・メモリに読み出して演算処理装置で実行させることができる。

【 0 0 1 8 】

本発明の第 3 の態様では、第 1 の記憶手段はコンピュータの主電源が停止している状態で記憶保持できるので、セキュリティ装置の装着についての設定が消去されることはない。また第 2 の記憶手段は、主電源が停止しかつ副電源が作動し

ている状態で記憶保持が可能である。この副電源は、上記のように電池や省エネ・モードによる電源を選定でき、より広範囲の素子や回路を利用できる。

【0019】

本発明の第4の態様では、内蔵基本電源により作動する連結手段で内蔵基本電源線を連結する。これにより内蔵基本電源線からの電力供給線を確保できる。コンピュータにセキュリティ装置が装着されて内蔵基本電源の電力供給路を形成しているときには連結手段の連結を遮断する。これはセキュリティ装置による電力供給路が形成され、連結手段の連結が2重の連結になるからである。この連結の遮断は維持され、この状態でセキュリティ装置が脱着されると、内蔵基本電源の電力供給が絶たれるので、内蔵基本電源の電力供給により保持されていた情報例えば設定情報やパスワードが消去され、コンピュータへのアクセスが禁止される。

【0020】

本発明のセキュリティ装置は、デバイス・ベイの蓋部に組み込むことで、コンピュータの余分なスペースを消費することなくオプション部品とすることができ、デバイス・ベイの蓋は、セキュリティ装置を組み込んだ蓋とセキュリティ装置を組み込んでいない単なる蓋の二つをオプション部品としていずれか一つを選択できるようにし、ユーザまたは販売店でコンピュータに装着できる。このセキュリティ部品には、RFアンテナやジャンパ等の接続部材を含んでいる。

【0021】

【発明の実施の形態】

[コンピュータ・システムの概要]

図1には、本発明を実施するのに適した典型的なノート型パーソナル・コンピュータ10のハードウェア構成をサブシステム毎に模式的に示している。CPU11は、OSの制御下で、各種プログラムを実行するようになっている。CPU11は、システム・バス13を経由して、一般にメモリ/PCI制御チップ15と呼ばれるブリッジ回路（ホスト-PCIブリッジ）に接続されている。本実施例のメモリ/PCI制御チップ15は、メイン・メモリ17へのアクセス動作を制御するためのメモリ・コントローラ機能や、システム・バス13とPCIバス

19間のデータ転送速度の差を吸収するためのデータ・バッファなどを含んだ構成となっている。

【0022】

メイン・メモリ17は、CPU11の実行プログラムの読み込み領域として、あるいは実行プログラムの処理データを書き込む作業領域として利用される、書き込み可能メモリである。ここで言う実行プログラムには、Windows98などのOS、周辺機器類をハードウェア操作するための各種デバイス・ドライバ、特定業務に向けられたアプリケーション・プログラムや、FLASH ROM 49に格納されたBIOSが含まれる。ビデオ・サブシステム21は、ビデオに関連する機能を実現するためのサブシステムであり、CPU11からの描画命令を実際に処理し、処理した描画情報をビデオ・メモリ（VRAM）に一旦書き込むとともに、VRAMから描画情報を読み出して液晶ディスプレイ（図示せず。）に描画データとして出力するビデオ・コントローラを含む。

【0023】

カードバス・コントローラ23は、PCIバス19のバス・シグナルをPCIカード・スロット25のインタフェース・コネクタ（カードバス）に直結させるための専用コントローラである。PCIバス19とI/Oバス39とは、多機能PCIデバイス27によって相互接続されている。本実施例の多機能PCIデバイス27は、PCIバス19とI/Oバス39とのブリッジ機能、DMAコントローラ機能、プログラマブル割り込みコントローラ（PIC）機能、及びプログラマブル・インターバル・タイマ（PIT）機能、IDE（Integrated Drive Electronics）インタフェース機能、USB（Universal Serial Bus）機能、SMB（System Management Bus）インタフェース機能を備えており、たとえば、インテル社より提供されているPIIX4というデバイスを選択することができる。IDEインタフェースには、IDEハードディスク・ドライブ（HDD）31が接続される他、IDE CD-ROMドライブ32が接続される。また、IDE CD-ROM32ドライブの代わりに、DVD（Digital Video Disc又はDigital Versatile Disc）ドライブのよ

うな他のタイプのIDE装置が接続されていても良い。HDD 31やCD-ROMドライブ 32のような外部記憶装置は、例えばシステム10本体内の「メディア・ベイ」又は「デバイス・ベイ」と呼ばれる収容場所に格納される。これら標準装備された外部記憶装置は、FDDやバッテリー・パックのような他の機器類と交換可能かつ排他的に取り付けられる場合もある。

【0024】

多機能PCIデバイス27にはRFIDタグとしての機能を発揮するRFIDチップ33が接続される。RFIDチップ33にはRFアンテナ37、第1短絡素子36及び第2短絡素子38が接続される。RFアンテナ37、第1短絡素子36及び第2短絡素子38は、HDD 31をコンピュータ10に収納するためのデバイス・ベイの蓋部に組み込まれている。セキュリティ機能を必要としないユーザは、RFアンテナ37が組み込まれていないデバイス・ベイの蓋を選択することができる。すなわち、セキュリティ装置の一部としてのRFアンテナ37、第1短絡素子36及び第2短絡素子38はオプション部品であり、ユーザ自らがまたは販売店において、RFアンテナ37、第1短絡素子36及び第2短絡素子38が付加されたアンテナ付き蓋またはアンテナ無し蓋のいずれか一方を装着することができる。RFIDチップ33は、リーダ/ライタが発信したRF励振信号をRFアンテナ37で受信して処理し、コンピュータの不正な持ち出しや不正なアクセスを禁止するセキュリティ機能を備えている。

【0025】

また、本実施例では、RFIDチップ33には、セキュリティ機能をより強固なものとするためにリチウムバッテリー34に接続されている。このリチウムバッテリー34は、周知のように、システムメモリ領域に現在のシステム構成情報を保持するメモリ（所謂CMOSメモリ）50を不揮発性とするために電力を供給したり内蔵時計をバックアップするために電力を供給したりするため、通常交換が困難なバッテリー電源である。これらの要素はコンピュータ10のセキュリティ機能の一部を分担しており、後に動作の概要を説明する

I/Oバス39としては、例えばISAバスがあり、Super I/Oコントローラ41、電源コントローラ45、FLASH ROM49、メモリ（所謂

CMOSメモリ) 50等が接続される。Super I/Oコントローラ41は、フロッピー・ディスク・ドライブ(FDD)の駆動、パラレル・ポートを介したパラレル・データの入出力(PIO)、シリアル・ポートを介したシリアル・データの入出力(SIO)を制御するための周辺コントローラで、I/Oポート43が接続される。電源コントローラ45は主としてシステム内のパワー・マネジメントやサーマル・マネジメントを行うシングル・チップ・マイコンで、日立製作所から提供されるH8/300チップを選定することができる。電源コントローラ45は、MPU、RAM、ROMおよびタイマ等を備え、ROMにはパワー・マネジメントやサーマル・マネジメントを実行するのに必要なプログラムおよび参照テーブルを格納している。電源コントローラ45には、パワー・サプライ・コントローラ47が接続されている。パワー・サプライ・コントローラ47にはバッテリーを充電するための充電器およびコンピュータ10で使用する5V、3.3V等の一定電圧を生成するためのDC/DCコンバータが含まれ、電源コントローラ45のもとで直接的に電力制御を行う。

【0026】

FLASH ROM49は、キーボードやフロッピー・ディスク・ドライブ(FDD)などの各ハードウェアの入出力操作を制御するためのコード群(BIOS: Basic Input/Output system)や、電源投入時の自己診断テスト・プログラム(POST: Power On Self Test)などのファームウェアを恒久的に格納するための書き換え可能な不揮発性メモリである。メモリ(所謂CMOSメモリ)50は、システムメモリ領域に現在のシステム構成情報を保持するためにリチウムバッテリー34から電力が供給されるメモリである。なお、コンピュータ・システム10を構成するためには、図1に示した以外にも多くの電気回路等が必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。

〔RFIDを利用したセキュリティ機能〕

RFIDとは一般にRF(Radio frequency)すなわ無線を使ってID(identifier)をEEPROMに読み書きする機能であるとい

うことができる。RFIDは単に無線を使った情報交換にとどまらず、一方にリーダー/ライタを配置し他方にRFIDタグを配置した場合に両者間で情報交換するためにRFIDタグが電源を必要としないところに最大の特徴がある。リーダー/ライタはRFIDタグにRF励振信号を送り、RFIDタグを励振して電力を発生させてデータを書き込みまたその電力を利用してRFIDタグがデータをリーダー/ライタに送り返す。このようなRFIDによるデータの読み書き機能を利用して、電源が停止したコンピュータとリーダー・ライタとの間で多くの情報を交換することができコンピュータの在庫管理等に利用できる。

【0027】

RFIDの他の利用形態としてコンピュータのセキュリティ機能に関するものがある。図2は、RFIDタグとしてのRFIDチップ33の内部構成を概略的に記載したものである。このようなRFIDチップとしては、ATMEL社から提供されるAT24RF08という型式のEEPROM (Asset identification EEPROM) がある。RFIDチップ33に含まれるEEPROM55は、記憶領域が8Kビットの一般エリア57と256ビットの特殊エリア59に分割されている。一般エリア57には、RFアンテナ37で受信したRF励振信号のデータがアナログ・インタフェース53を経由して書き込まれ、また書き込まれているデータはインタフェース53およびRFアンテナ37を経由して発信される。またEEPROM55とコンピュータ10はシリアル・インタフェース61およびSMB35を通じて通信し、コンピュータから一般エリア57および特殊エリア59への書き込みおよび読み出しができる。

【0028】

ここで、特殊エリア59には1つの記憶領域が設けられている。それは、RFアンテナの装着検出の設定を示すRemoval Detect Enableビットである。このRemoval Detect Enableビットは、予め用意されたセットアップユーティリティでオプションパーツとしてRFアンテナを装着するときに設定するものであり、適切なパスワードを保有するユーザが設定することにより、「1」がセットされる。なお、初期状態すなわち未装着のときは「0」すなわちリセットされている。一般エリア57には、2つの記憶領

域が設けられている。その一つは、RFアンテナの装着状況の履歴を示す Antenna Historyビットで、コンピュータ10へRFアンテナが装着されたことが検出されると「1」にセットされる。もう一つは、Antenna Errorビットで、一旦装着されたRFアンテナ37が脱着されたことが検出されると「1」にセットされる。Removal Detect Enableビット、Antenna HistoryビットおよびAntenna Errorビットは適切なパスワードを保有するユーザがSMB35およびシリアル・インタフェース61を経由してコンピュータ・システムからEEPROM55にアクセスしない限りリセットできない。

【0029】

特殊エリア59には、RFアンテナ37のコンピュータ10に対する着脱状態を検出するためのDE/DCビット領域、RFアンテナ37が監視区域のゲード近くに設置されたリーダ/ライタからRF励振信号を受信したときにセットするTamperビット領域、一般エリア57へのリード、ライトをロックするAccess Protectionビット領域、およびコンピュータの電源がオフになるまでAccess Protectionビットの変更をロックするStickyビット等が含まれる。Access Protectionビットは2ビットで構成され、「00または01」のときは一般エリアへの一切のアクセスが禁止され、「10」のときは読み出しだけが許可され、「11」のときは書き込みおよび読み出しが許可される。

【0030】

DE/DCビット領域は、DEビット(Detect Enable bit)とDCビット(Detect Coil bit)からなる。RFIDチップ33は、シリアル・インタフェース61を通じてDEビットが「1」にセットされるとRFアンテナ37の着脱状態をチェックし、RFアンテナ37が装着されているときは「1」を、脱着されているときは「0」をDCビットに書き込むようになっている。コンピュータの電源が入っている場合は電源部51がアナログ・インタフェース53を駆動するが、電源がない場合はRFアンテナ37を通じて受信したRF励振信号がアナログ・インタフェース53を駆動し、電源がない

状態でもリーダー/ライターと通信できる。

【0031】

また、本実施例では、RFIDチップ33は、デジタルインタフェース62を含んでいる。デジタルインタフェース62は、NAND素子63、フリップフロップ回路65、アナログスイッチ67を含んでおり、特殊エリア59に書き込まれているRemoval Detect Enableビットの状態（「1」または「0」）がハイレベル信号またはローレベル信号として、アナログスイッチ67の制御側及びNAND素子63の一方の入力側に出力される構成になっている。NAND素子63の他方の入力側はフリップフロップ回路65を介して端子71に接続されている。本実施例では、フリップフロップ回路65として所謂Dフリップフロップを用いており、入力側（D端子）に端子71が接続され、不論理出力側（／Q端子）にNAND素子63の他方の入力側が接続されている。このフリップフロップ回路65の入力側（D端子）と端子71の間は抵抗69を介して電源に接続されている。端子71と一対である端子73は接地されており、第1短絡素子36の接続で端子71と端子73とが短絡する。これにより、フリップフロップ回路65の入力側（D端子）は、第1短絡素子36が接続されることでローレベルとなり、離間することによりハイレベルとなる。なお、図示は省略したが、フリップフロップ回路65にはシステムクロック及びリセット信号が入力されるように接続されている。NAND素子63の出力側は、第1短絡素子36の接続状態（接続又は離間）を出力するために、電源コントローラ45に接続されている。このNAND素子63の出力信号は、後述するキーボード等の入力操作を禁止するためのINTR信号として機能する。なお、NAND素子63、上記フリップフロップ回路65、及び抵抗69へ電力を供給する電源は、電源コントローラ45の基の電力制御に連動し、電源投入後はもとより、所謂スタンバイ時、サスペンド時のように電力の消費を抑制する省電力モード時にも電力が供給されるものとする。

【0032】

アナログスイッチ67の一方の端子はリチウムバッテリー34のプラス側に直接接続され端子77に接続されている。端子77と一対である端子75は、リチ

ウムバッテリー 34 に直接接続されるべき、上記システム構成情報を保持するメモリ（所謂 CMOS メモリ）50 の電源に接続されると共に、アナログスイッチ 67 の他方の端子が接続される。Removal Detect Enable ビットの状態が「1」であるときは、アナログインタフェース 53 を介してハイレベル信号がアナログスイッチ 67 に供給されて、アナログスイッチ 67 は非導通となる。これにより、CMOS メモリにはアナログスイッチ 67 を介してのリチウムバッテリー 34 の電力供給がされることはない。一方、Removal Detect Enable ビットの状態が「0」であるときは、ローレベル信号がアナログスイッチ 67 に供給されて、アナログスイッチ 67 は導通する。これにより、CMOS メモリとリチウムバッテリー 34 とはアナログスイッチ 67 を介して導通電されることになる。従って、Removal Detect Enable ビットの状態が「1」であるときは、第 2 短絡素子 38 の接続で端子 75 と端子 77 とが短絡することにより、CMOS メモリにはリチウムバッテリー 34 の電力供給がなされ、第 2 短絡素子 38 の離間により CMOS メモリへのリチウムバッテリー 34 の電力供給が遮断される。なお、アナログスイッチ 67 にはリチウムバッテリー 34 から直接電源供給されており、システムの電源状態に関わらずスイッチ状態を維持できるものとする。また、本実施例では、ハード構成を用いて説明するが、本発明はこれに限定されるものではなく、ソフトウェア構成でもよい。

[本発明の実施例を適用するセキュリティ機能の概要]

次に本発明の実施例を適用するコンピュータのセキュリティ機能の概要を説明する。電源がオフになっているコンピュータが監視区域のゲートに近づくと、リーダー/ライターが発信する RF 励振信号が RF アンテナ 37 に送られ、EEPROM 55 の特殊エリア 59 に Tamper ビットがセットされる。つぎにコンピュータの電源を投入すると、FLASH ROM 49 に格納されている BIOS がメイン・メモリ 17 に書き込まれ、CPU 11 は POST およびシステムの初期化を実行する。POST が Tamper ビットを検出するとパスワードの入力をユーザに要求すると共にその時点で POST の実行を停止し、パスワードの入力がない限りコンピュータへアクセスすることはできなくなる。

【0033】

前述のようにRFアンテナ37はユーザまたは販売店が装着できるようにしているため、不正にコンピュータを外に持ち出そうとする者がRFアンテナ37を外してからゲートを通過し、Tamperビットがセットされるのを回避しようとする可能性がある。本発明の実施例では、RFアンテナ37はオプションとして取り付けるが、その他のハードウェアはRFアンテナ37を装着する場合と脱着する場合とで共通である。また、RFアンテナ37を装着する場合とRFアンテナを脱着する場合のいずれにおいても同一のソフトウェア（BIOS）を採用できる。以下において、RFアンテナ37が脱着された場合にコンピュータへのアクセスを禁止するための手順の実施例を説明する。

【0034】

〔基本手順を示す例〕

まず、本発明の実施例を説明するのに先だって、電源がオフの状態でRFアンテナが不正に外された後、そのまま電源がオンにされた場合にコンピュータへのアクセスを禁止するための基本手順を説明する。

【0035】

図3は電源がオンの状態でRFアンテナが外された後、そのまま電源がオンにされた場合にコンピュータへのアクセスを禁止する基本手順を含むフローチャートである。コンピュータ10にRFアンテナが実際に装着されてセキュリティ機能が有効になるか否かは、この時点でシステムにとって不明である。コンピュータ10のAntenna HistoryビットおよびAntenna Errorビットは、工場から出荷する時点では共に「0」にセットされている。ブロック101でコンピュータ10の電源をオンにすると、BIOSがFLASH ROM49からメイン・メモリ17に読み出され、CPU11がPOSTプログラムを読みとって以下の手順を実行する。RFIDチップ33は、電源投入時点では常にAccess Protectionビットが「11」にStickyビットが「1」にセットされ、一般エリア57へのBIOSによるアクセスが許可される。ブロック103でPOSTは現実にはRFアンテナ37がコンピュータに装着されているか否かを確認するために特殊エリア59のDEビットを「1」

にセットする。これに応じてRFIDチップ33はRFアンテナ37の装着状態をチェックし、装着されていればDCビットに「1」を脱着されていれば「0」を書き込む。

【0036】

POSTはDEビットを「1」にセットしてから約200マイクロ秒経過した後DCビットを読みとり、さらにDEビットを「0」にセットする。DCビットが「1」にセットされて現在RFアンテナ37が装着されていることが確認されたならばブロック105に移行して一般エリア57のAntenna Historyビットを「1」にセットする。この時点で、コンピュータ10がセキュリティ機能を具備するコンピュータであることがシステムによって認識されたことになり、以後Antenna Historyビットは、パスワードを有するユーザが書き換ええない限り電源がオフになってもこの情報を維持し続ける。DCビットが「0」でRFアンテナが脱着されていることが確認されたならば、ブロック107に移行して一般エリア57のAntenna Errorビットを確認する。Antenna Errorビットをこの時点で確認することは、後にブロック109で詳細に説明するが、前日のPOSTを実行する以前に一旦装着されたRFアンテナが脱着されたことがあったか否かを確認することに相当する。

【0037】

ブロック107でAntenna Errorビットが「1」のときは、前回のPOSTを実行する以前にRFアンテナ37が一旦装着され、さらに前日のPOSTを実行する段階でRFアンテナ37が脱着されていた場合であり、RFアンテナの不正な脱着があったものとしてこれを処理するブロック119に移行する。以後Antenna Errorビットは、パスワードを有するユーザが書き換ええない限り電源がオフになってもこの情報を維持し続ける。ブロック107でAntenna Errorビットが「0」のときは、すくなくとも前日のPOSTの実行時点まではRFアンテナの不正な脱着がなかったものと判断し、ブロック111に移行する。

【0038】

ブロック111では、Antenna Historyビットを確認する。す

なわち、今回のPOSTを実行する時点までにRFアンテナ37がコンピュータ10に装着されたことがあるか否かを確認する。Antenna Historyビットへのデータは、ブロック105により今回のPOST実行時に、または前日以前のPOST時に書き込まれる。ブロック111でAntenna Historyビットが「0」のときは、現在までRFアンテナが装着されたことがない場合であってコンピュータ10はセキュリティ機能を有しないコンピュータであることを意味しており、ブロック115に移行する。ブロック111でAntenna Historyビットが「1」のときは、今回のPOSTを実行する時点までにRFアンテナが装着されたことがあり、かつ前回のPOSTを実行する時点までの間に一旦装着されたRFアンテナが脱着されたことがPOSTで検出されていない場合（Antenna Errorビット=0）であり、ブロック113に移行する。

【0039】

ブロック113ではDCビットを再度確認し、今回のPOST実行時点でRFアンテナ37が装着されているか脱着されているかを判断する。DCビットが「1」すなわち現実にRFアンテナ37がコンピュータ10に装着されていれば、セキュリティ装置の脱着はなかったものとしてブロック115に移行する。DCビットが「0」のときは、今回のPOSTを実行する以前にRFアンテナが装着されていたが（ブロック111）今回のPOSTを実行する段階では脱着されており（ブロック113）、さらに前回のPOSTを実行する以前に一旦装着されたRFアンテナが前回以前のPOSTを実行する段階で脱着されたことが検出されていない（ブロック107）場合であり、ブロック109に移行して処理される。言い換えると、これは前回のPOSTを実行してから今回のPOSTを実行するまでの間にRFアンテナが脱着された場合を今回のPOSTで処理する手順である。前回のPOSTを実行する時点においてそれまでに一旦装着されたRFアンテナ37が脱着されていると、前回のPOSTを実行する時点でAntenna Errorビットが「1」にセットされ、今日のPOSTを実行するとブロック107からブロック119に移行して処理されるからである。

【0040】

ブロック 115 は、ブロック 111 から移行する手順で示されるセキュリティ機能を有しないコンピュータと、ブロック 113 から移行する手順で示されるセキュリティ機能を有しかつ RF アンテナ 37 が一旦装着された後に脱着されたことがないコンピュータとを処理する。この場合は、セキュリティ装置の脱着はないので、Access Protection ビットを「10」にセットし、以後一般エリアの Antenna History ビットおよび Antenna Error ビットへの書き込みを禁止する。さらに Sticky ビットを「0」にセットして、コンピュータの電源が切られるまで Access Protection ビットの変更ができないようにする。これは、OS 経由で Access Protection ビットが「11」に変更され、Antenna History ビットまたは Antenna Error ビットの内容が書き換えられるのを防止するためである。この結果 Antenna History ビットおよび Antenna Error ビットの書き換えは、電源がオンになったブロック 101 からブロック 115 までの間だけ可能になり、実際はこの間に POST だけがビットの書き換えをすることになる。続いてブロック 117 に移行し、BIOS はブートストラップを実行し、OS およびアプリケーション・プログラムをメイン・メモリに読み出しコンピュータの構成を行う。

【0041】

ブロック 109 では Antenna Error ビットを「1」に書き換える。Antenna Error ビットは POST を実行する毎にブロック 107 ないしブロック 113 が判断され、その結果に応じて「1」に書き換えられる。ブロック 109 は、前日の POST を終了した時点では Antenna Error ビットが「1」に書き換えられていなかったが（ブロック 107）、今回の POST を実行した時点で過去において RF アンテナ 37 が装着されたことがある（ブロック 111）にも係わらず現在それが脱着されている（ブロック 113）場合を処理する。

【0042】

続いてブロック 109 からブロック 119 に移行する。さらにブロック 107 で判断した Antenna Error ビットが「1」である場合もブロック 1

19に移行する。ブロック119では今回のPOSTを実行する間にブロック109によりAntenna Errorビットが「1」にセットされた場合および前回のPOSTを終了するまでの間にAntenna Errorビットが「1」であったことに応答してコンピュータ10のディスプレイにPOSTエラーの表示をする。

【0043】

次にブロック121でディスプレイにユーザにパスワードを要求するメッセージを表示し、BIOSがブロック123で正しいパスワードの入力を認識すると、ブロック127でAntenna HistoryビットおよびAntenna Errorビットを「0」に書き換える。続いてブロック129でPOSTを再スタートする。再スタートしたPOSTでは、POSTエラーの表示ができることはなくブロック101からブロック117までの手順をクリアしてブートストラップが実行される。

【0044】

BIOSがブロック123で正しいパスワードを認識しないとその時点でPOSTは停止し、以後コンピュータへのアクセスはできなくなる。それ以降正しいパスワードを入力できる場合は、再度ブロック101の電源オンからスタートして、ブロック121で正しいパスワードを入力してからブロック129を経由して再度ブートストラップを実行する。

【0045】

ところで、上記図3のフローチャートで説明した手順では、電源がオンの状態でRFアンテナが不正に外されてコンピュータが外部に持ち出されても、一旦電源をオフにしてPOSTを実行する段階にならないとコンピュータへのアクセスを禁止することはできない。電源オンの状態でRFアンテナが外されてしまうことに対処するためには、図4に示すフローチャートにより達成できる。電源が投入され、図3で説明した手順でPOSTが実行されてブートストラップが開始されると、デバイス・ドライバによってブロック151から手順が開始される。ブロック153ではAntenna Historyビットが確認される。今回のPOSTを実行する時にRFアンテナが装着されていれば図3のブロック105

でAntenna Historyビットは「1」にセットされている。ブロック153では、Antenna Historyビットを確認し、ビットが「0」でRFアンテナが装着されていなければブロック157へ移行し本手順は終了する。

【0046】

ブロック153で確認したビットが「1」で今回のPOSTを実行した時点でRFアンテナが装着されていれば、ブロック155に移行する。ブロック155でポーリングにより定期的にDCビットの状態を確認する。このポーリングは実際には他のプログラムの実行を妨げないように、タイマー・インターラプトなどによって行われることが好ましい。RFアンテナ37が脱着されない限りCPUはRFアンテナの装着状態を定期的に監視する。RFアンテナ37が脱着されるとブロック159に移行しコンピュータの電源が強制的にオフにされるので、ユーザが再度電源をオンにすると図3に示したPOSTが再スタートさせられる。図3の手順ではブロック103、107、111、113、109、119、121のルートに従って処理され、パスワードが要求される。すなわちコンピュータの電源オンの状態において、一旦装着されたRFアンテナ37が脱着されると、CPU11のポーリングのタイミングでコンピュータの電源がオフにされるので、次の電源をオンにしたときPOSTが実行され、パスワードを入力できないユーザはそれ以上コンピュータにアクセスできないことになる。

【0047】

〔本発明の手順を示す第1の実施例〕

上記基本手順では、電源がオンの状態でRFアンテナが不正に外されたときについて、コンピュータへのアクセスを禁止する場合を説明した。本実施例では、スタンバイやサスペンドといわれるような各種省エネ・モード状態でRFアンテナが外されてしまうことに対処するためのものである。本発明の手順を示す第1の実施例としてのフローチャートを図5に示す。

【0048】

図5は本発明の手順を示す第1の実施例としてのフローチャートである。コンピュータ10の電源をオンにすると、BIOSがFLASH ROM49からメ

イン・メモリ17に読み出され、CPU11がPOSTプログラムを読みとって以下の手順を実行する。まず、ブロック81で予め用意されたセットアップユーティリティによりオプションパーツのセキュリティ機能を有効にする設定(Removal Detect Enableビット=1)がなされているか否かを判断する。セキュリティ機能無効の設定の場合には、コンピュータへのアクセスを禁止する必要がないため、ブロック81で否定され、本手順を終了する。なお、図5に示す手順は、定期的に行われるように実行させることができる。

【0049】

コンピュータ10にRFアンテナが実際に装着されても、セキュリティ機能を有効にするまでは、機能しない。そこで、適切なパスワードを保有するユーザは、コンピュータ10にRFアンテナが実際に装着されてセキュリティ機能を有効にするために、RFアンテナの装着開始を設定するにあたり、予め用意されたセットアップユーティリティでオプションパーツを設定する。これにより、Removal Detect Enableビットが「1」に設定される。この場合、ブロック81で肯定され、これにより、RFIDチップ33は、ハイレベル信号をアナログスイッチ67の制御側及びNAND素子63の一方の入力側に出力する。

【0050】

このとき、図2に示すように、第1短絡素子36の接続で端子71と端子73とが短絡している場合、フリップフロップ回路65の入力側(D端子)はローレベルで出力側はハイレベルである。従って、NAND63には共にハイレベル信号が入力され、出力であるINTR信号はローレベルである。一方、第1短絡素子36が離間されると、フリップフロップ回路65の出力側は1クロック送れてローレベルになる。従って、NAND63の出力であるINTR信号はハイレベルになる。すなわち、INTR信号がハイレベルになる場合には、第1短絡素子36が離間つまりRFアンテナ37が脱着されたことになる。そこで、ブロック85でPOSTはINTR信号(ハイレベル信号)が出力されたか否かを確認し、INTR信号がハイレベル信号であるとき、第1短絡素子36が脱着されているとして、ブロック87に移行してキーボードをロックし、入力不能とすること

によりコンピュータを停止させる。これにより、POSTは停止し、以後コンピュータへのアクセスはできなくなる。一方、INTR信号がローレベル信号であるとき、第1短絡素子36が装着されているとして、本手順を終了する。なお、上記図3で説明したブロック103へ進み、上述のようにして、電源オン時の手順を実行（ブーストラップ等が開始されたり継続中の処理が再開）してもよい。

【0051】

このように、電源コントローラ45の電力制御に連動し、電源投入後はもとより、所謂スタンバイ時、サスペンド時のように電力の消費を抑制する省電力モード時にも電力が供給されている場合に、第1短絡素子36が脱着されたすなわちRFアンテナ37が脱着された場合には、入力不能とすることによりコンピュータを停止させるので、RFアンテナ37が脱着された場合にコンピュータへのアクセスを禁止することができる。

【0052】

[本発明の手順を示す第2の実施例]

上記図5のフローチャートで説明した手順では、電源がサスペンド等の省エネモードの状態ではRFアンテナが外されたときについて、コンピュータへのアクセスを禁止する場合を説明した。本実施例では、機械的に電源オフ状態にした場合やハイパーネーションといわれるような基本構成部分のみの電源状態でRFアンテナが外されてしまうことに対処するためのものである。すなわち、図5のフローチャートで説明した手順では、電源が機械的に遮断または基本構成部分のみの最低電源状態でRFアンテナが外されてコンピュータが外部に持ち出し、再度RFアンテナを装着されると、コンピュータへのアクセスを禁止できない。本実施例は、これに対処するためのものである。本発明の手順を示す第2の実施例としてのフローチャートを図6に示す。

【0053】

本発明の手順を示す第2の実施例としてのフローチャートを図6に示す。コンピュータ10の電源をオンにすると、BIOSがFLASH ROM49からメイン・メモリ17に読み出され、CPU11がPOSTプログラムを読みとって以下の手順を実行する。まず、ブロック89で予め用意されたセットアップユー

ティリティによりオプションパーツのセキュリティ機能を有効にする設定がなされているか否かを判断する。セキュリティ機能無効の設定の場合には、コンピュータへのアクセスを禁止する必要がないため、ブロック 89 で否定され、本手順を終了する。なお、上記図 3 で説明したブロック 103 へ進み、上述のようにして、電源オン時の手順を実行（ブーストラップ等が開始されたり継続中の処理が再開）してもよい。

【0054】

上記説明したように、適切なパスワードを保有するユーザが、コンピュータ 10 に RF アンテナが実際に装着されてセキュリティ機能を有効にするために、Removal Detect Enable ビットが「1」に設定されると、ブロック 89 で肯定され、これにより、RFID チップ 33 は、アナログインタフェース 53 を介してハイレベル信号をアナログスイッチ 67 の制御側に出力する。これにより、ブロック 95 でアナログスイッチ 67 が作動され、端子 75 と端子 77 の間の導通が切断される。

【0055】

Removal Detect Enable ビットの状態が「1」であるときは、第 2 短絡素子 38 の接続で端子 75 と端子 77 とが短絡することにより、CMOS メモリにはリチウムバッテリー 34 の電力供給がなされ、第 2 短絡素子 38 の離間により CMOS メモリへのリチウムバッテリー 34 の電力供給が遮断される。すなわち、Removal Detect Enable ビットの状態が「1」のままで、第 2 短絡素子 38 が離間つまり RF アンテナ 37 が脱着されたときには、リチウムバッテリー 34 により供給されていた所謂 CMOS メモリへの電力が遮断される。このため、CMOS エラーが発生する。CMOS エラーが発生すると、次回の電源オン時に、上記ブロック 119 へ進み（図 3 に結合子 2 で示した）、ユーザにパスワードを要求する。このように、正しいパスワードの入力により、RF アンテナ 37 が脱着された場合にコンピュータへのアクセスを禁止することができる。

【0056】

一方、CMOS エラーが非発生の場合には、第 2 短絡素子 38 が正しく装着さ

れているものとして、上記図3の手順を実行し、電源がオフの状態ではRFアンテナが外されてそのまま電源がオンされた場合にコンピュータへのアクセスを禁止する手順を進める。すなわち、図3のブロック103から実行する。

【0057】

このように、本実施例では、電源がオフ状態や最小電力の省エネモードで稼働中のコンピュータで、RFアンテナ37が脱着された場合であっても、アナログスイッチでリチウムバッテリーからのCMOSへの電源供給を遮断できる。このため、着脱したRFアンテナを再度取り付けて、ユーザが再度電源をオンにしてPOSTが再スタートさせられた場合であっても、一旦装着されたRFアンテナ37が脱着されると、CMOSメモリへの電源がオフにされるので、次の電源をオンにしたときにはPOSTが実行され、パスワードを入力できないユーザはそれ以上コンピュータにアクセスできないことになる。

【0058】

図7に本発明を実行するコンピュータ10の外形の一例を示す。コンピュータ10は図1で説明した構成要素を収納する本体201、液晶ディスプレイ203、本体上部に配置したキーボード207、CD-ROMドライブ32、およびHDD31を収納するデバイス・ベイの蓋209を含む。コンピュータ10はデバイス・ベイの蓋209を除いて、本実施例との関連で特別な外形的特徴を備えるものではない。

【0059】

図8に本発明で使用するRFアンテナ37、第1短絡素子36及び第2短絡素子38の装着方法の実施例を示す。RFアンテナ37、第1短絡素子36及び第2短絡素子38はデバイス・ベイの蓋209に収納される。デバイス・ベイにHDD31が着脱可能な状態で装着した後に蓋209を本体201に対してはめ込み構造で取り付ける。RFアンテナ37、第1短絡素子36及び第2短絡素子38を使用しない場合、すなわちセキュリティ機能を必要としないコンピュータでは、RFアンテナ37を取り付けずに蓋209だけを本体201に装着できる。また、蓋209とは異なりRFアンテナ37、第1短絡素子36及び第2短絡素子38を収納できない構造の蓋を用意してもよい。このようなRFアンテナ3

7、第1短絡素子36及び第2短絡素子38の取り付け構造を蓋209に採用することにより、ユーザまたは販売店でRFアンテナ37、第1短絡素子36及び第2短絡素子38の取り付けが可能になり、ユーザはセキュリティ機能の必要性に応じてRFアンテナ37、第1短絡素子36及び第2短絡素子38付きの蓋209またはRFアンテナ37、第1短絡素子36及び第2短絡素子38なしの蓋209のいずれかを選択できる。蓋209の内側には、アンテナ37用コイルが収納され、そのリード部211は蓋209の端子部213にはめ込まれると共に、RFIDチップ33に電氣的に接続される。また、蓋209の端子部215には、第1のジャンパ端子として機能するリード部の第1短絡端子36がはめ込まれ、端子部217には、第2のジャンパ端子として機能するリード部の第2短絡端子38がはめ込まれる。

【0060】

このような方法でRFアンテナ37、第1短絡素子36及び第2短絡素子38を取り付ける場所としては、HDD用のデバイス・ベイの蓋部にとどまらずCD-ROMドライブ、DVDドライブ、FDD、バッテリ等の外部装置のデバイス・ベイの蓋や、これらを択一的に収納できるマルチ・ベイの蓋を利用できる。RFアンテナ37、第1短絡素子36及び第2短絡素子38の本体201に対する取り付け構造は、コンピュータの使用場所において不正行為者が短時間に脱着できるものではなく、かつ販売店またはユーザがある程度の時間を費やして着脱できる程度に強固なものであることが好ましい。たとえば、はめ込み構造に加えてスクリューで締め付ける構造や、そのスクリューに特殊な工具を要するものを採用することができる。

【0061】

本発明の実施例はRFIDを利用したセキュリティ装置の脱着が行われたときにコンピュータへのアクセスを禁止する例で説明したが、本発明の適用範囲はRFIDに限定されるものではなく、たとえば指紋によりコンピュータへのアクセス資格を確認するような他の種類のセキュリティ装置にも適用できる。

【0062】

以上、本発明を特定の実施例に基づいて説明したが、本発明は、本発明の思想

を考慮して当業者が容易に考えることができるさらに多くの実施例を含むものである。

【0063】

【発明の効果】

本発明により、セキュリティ装置が脱着されたときにアクセスができなくなるコンピュータを提供することができた。また本発明により、装着および脱着が可能で余分なスペースを必要としないセキュリティ装置の取り付け構造を備えたコンピュータを提供することができた。

【図面の簡単な説明】

【図1】

本発明を実施するコンピュータの概略ブロック図の一例である。

【図2】

本発明め実施例で使用するRFIDチップの概略ブロック図である。

【図3】

本発明の手順を示す第1の実施例のフローチャートである。

【図4】

基本手順を補足する手順示す例のフローチャートである。

【図5】

本発明の手順を示す第1の実施例のフローチャートである。

【図6】

本発明の基本手順を示す例のフローチャートである。

【図7】

本発明を実施するコンピュータの外形図の一例である。

【図8】

本発明の実施例で使用するRFアンテナの取り付け方法の一例を示す図である。

【符号の説明】

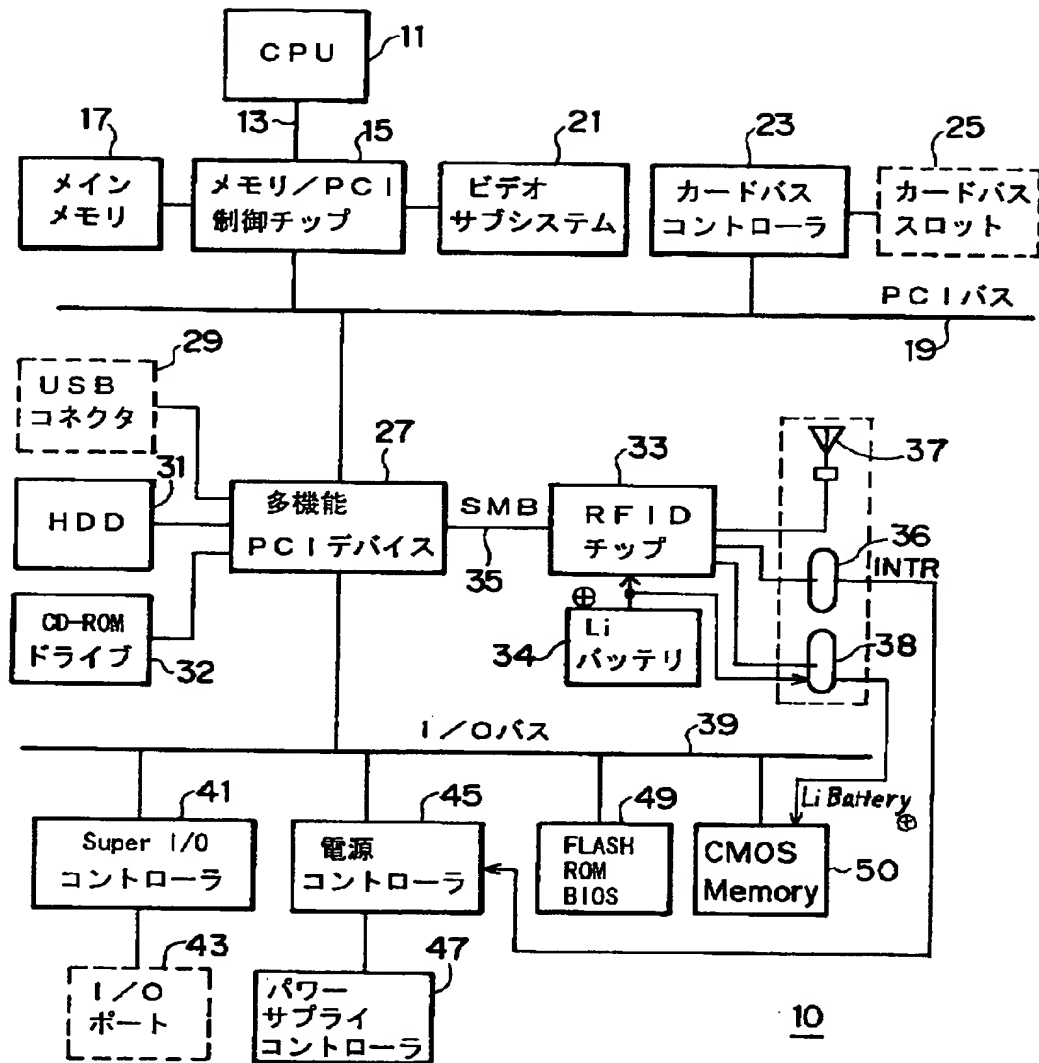
33 RFIDチップ

34 リチウムバッテリー

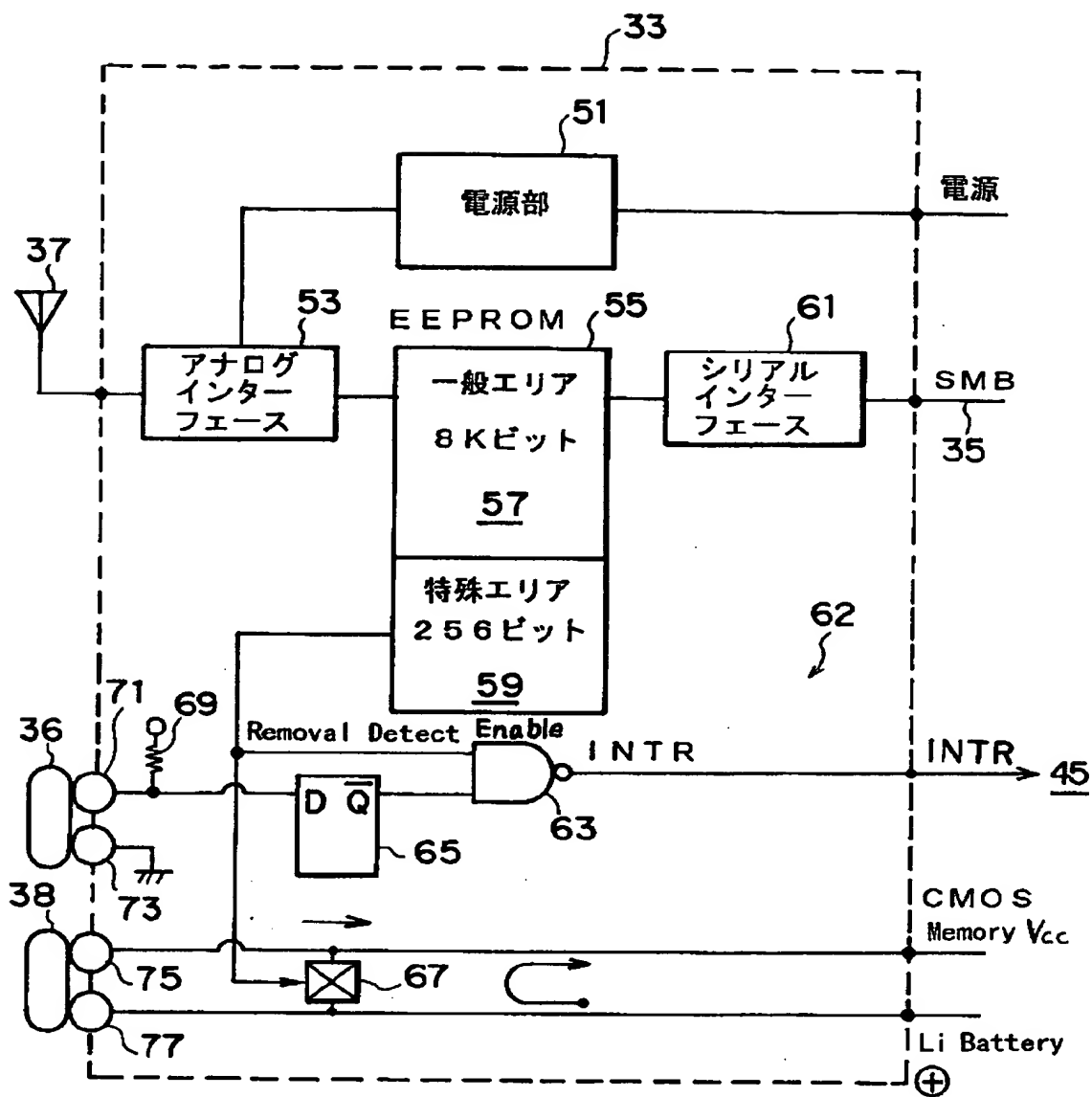
- 3 6 短絡素子
- 3 7 アンテナ
- 3 8 短絡素子
- 5 5 E E P R O M
- 6 1 シリアルインタフェース
- 6 2 デジタルインタフェース
- 6 3 N A N D 素子
- 6 5 フリップフロップ回路
- 6 7 アナログスイッチ
- 6 9 抵抗

【書類名】 図面

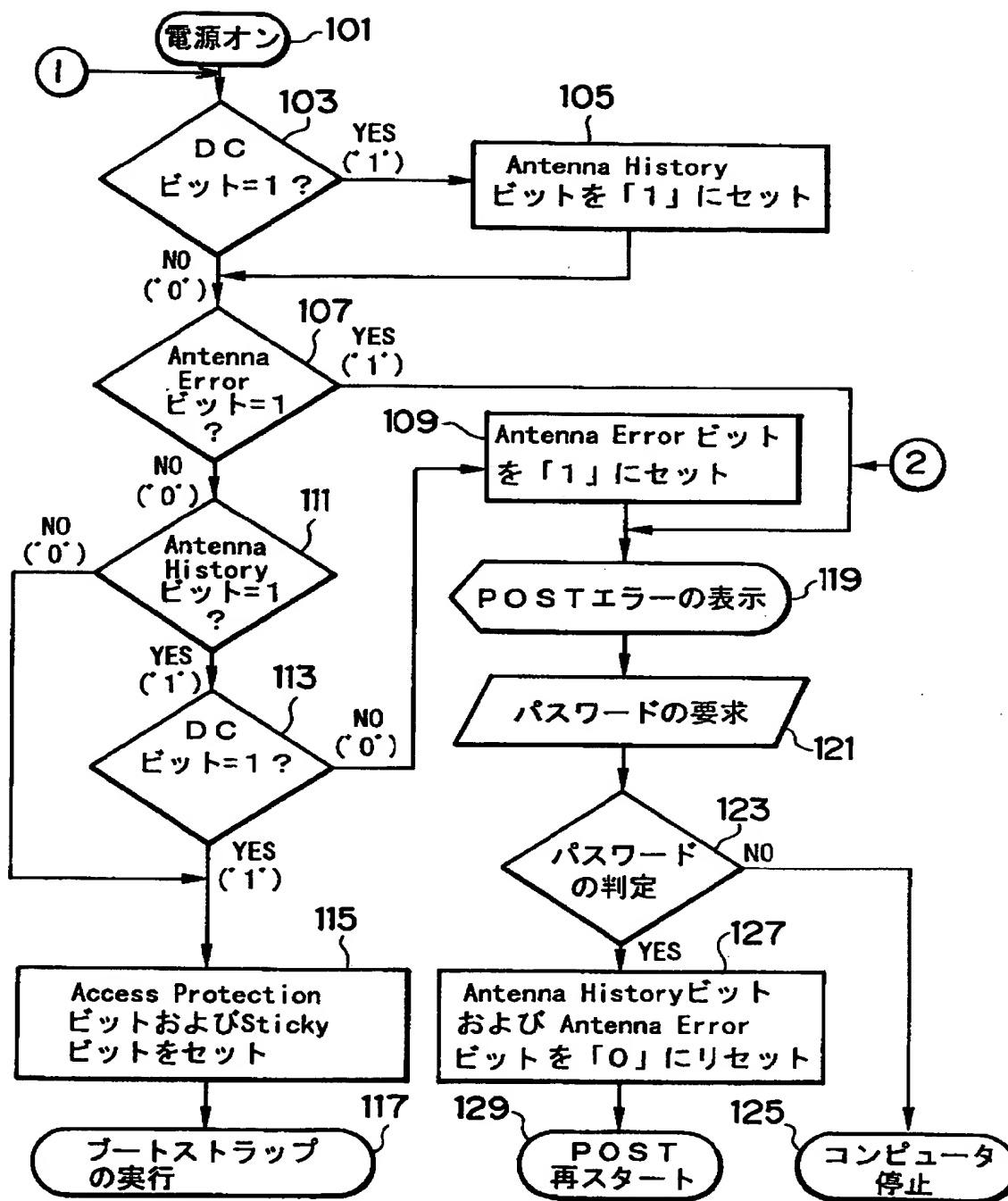
【図 1】



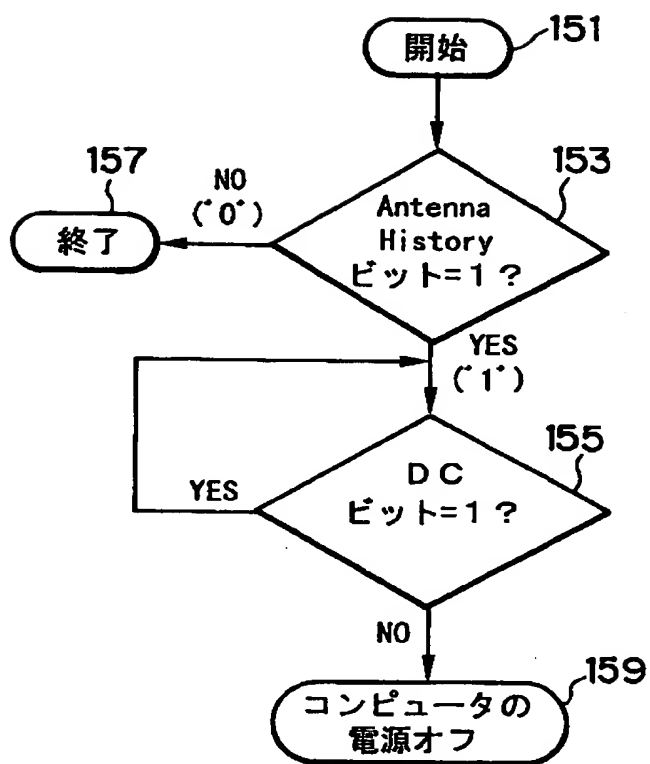
【図 2】



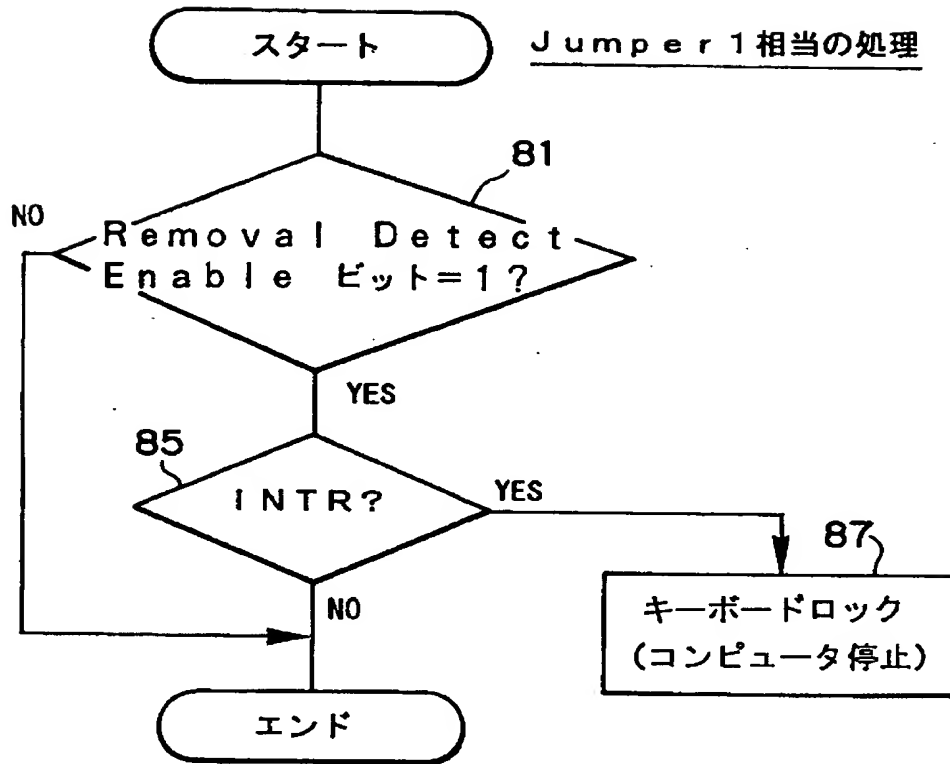
【図 3】



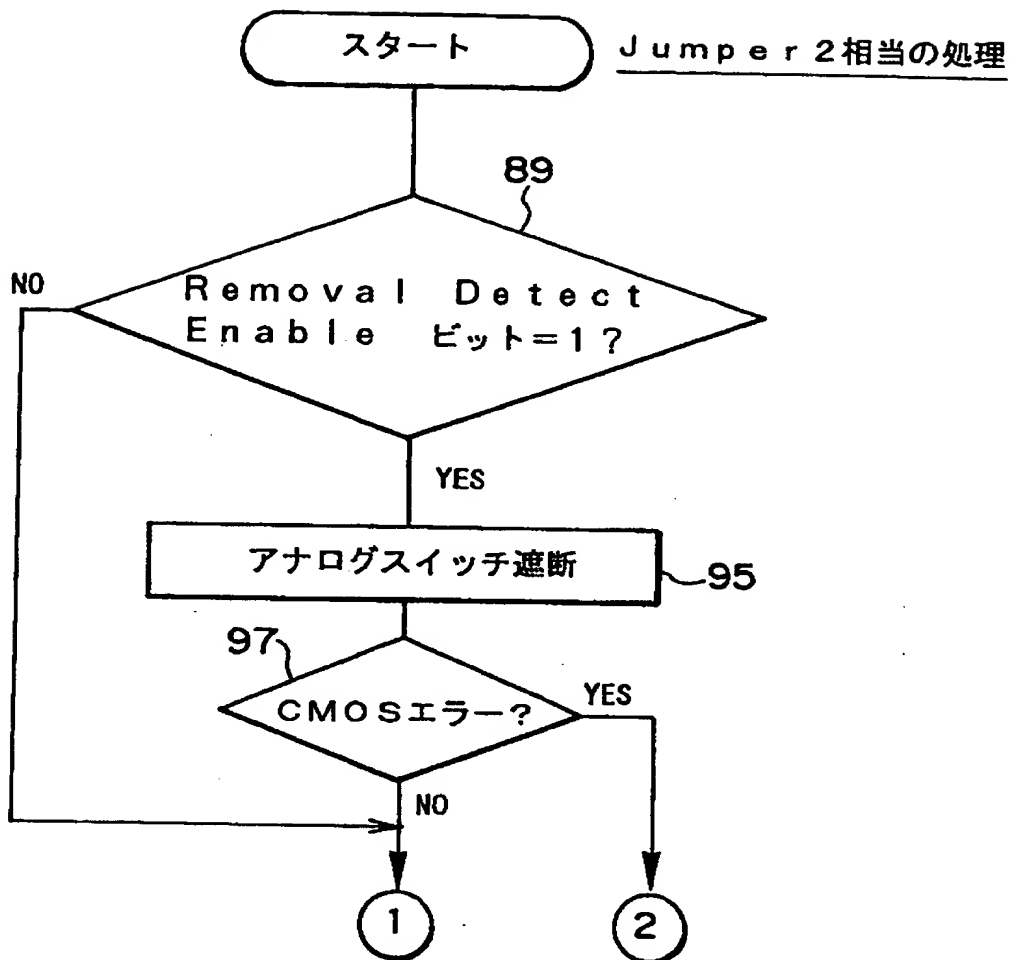
【図 4】



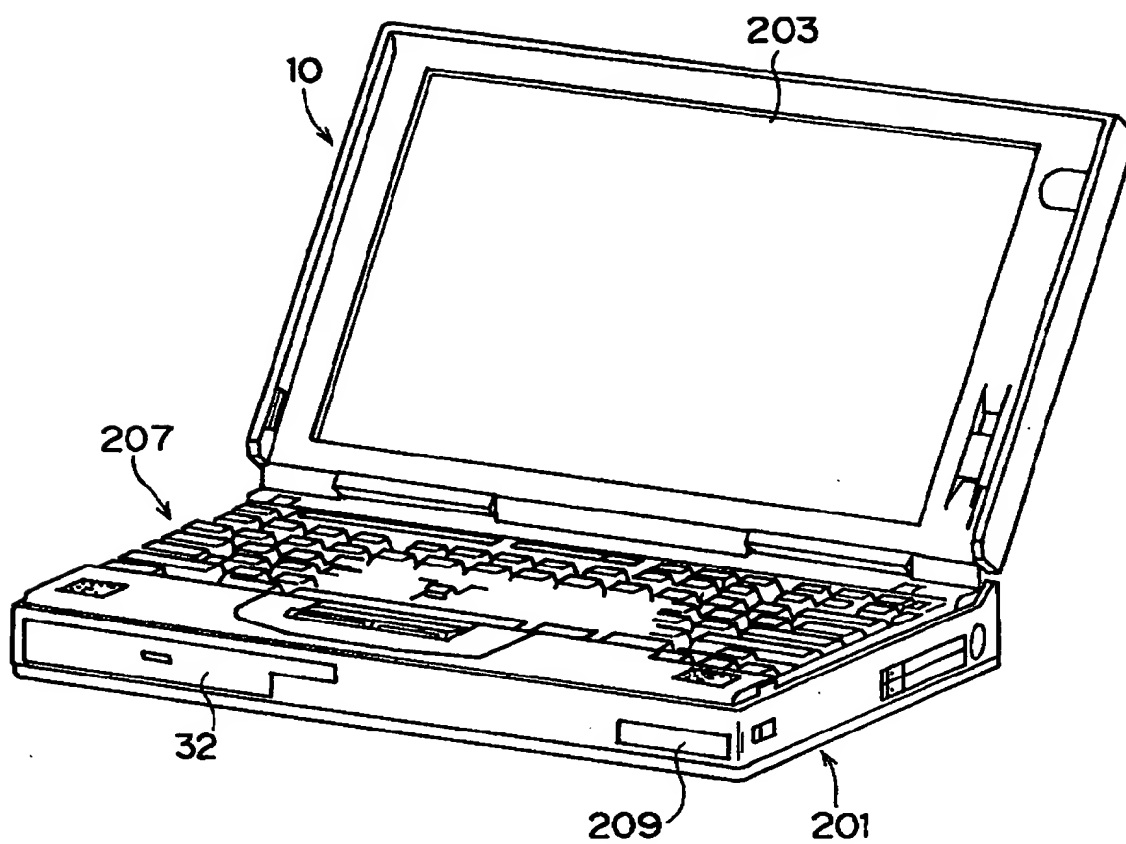
【図 5】



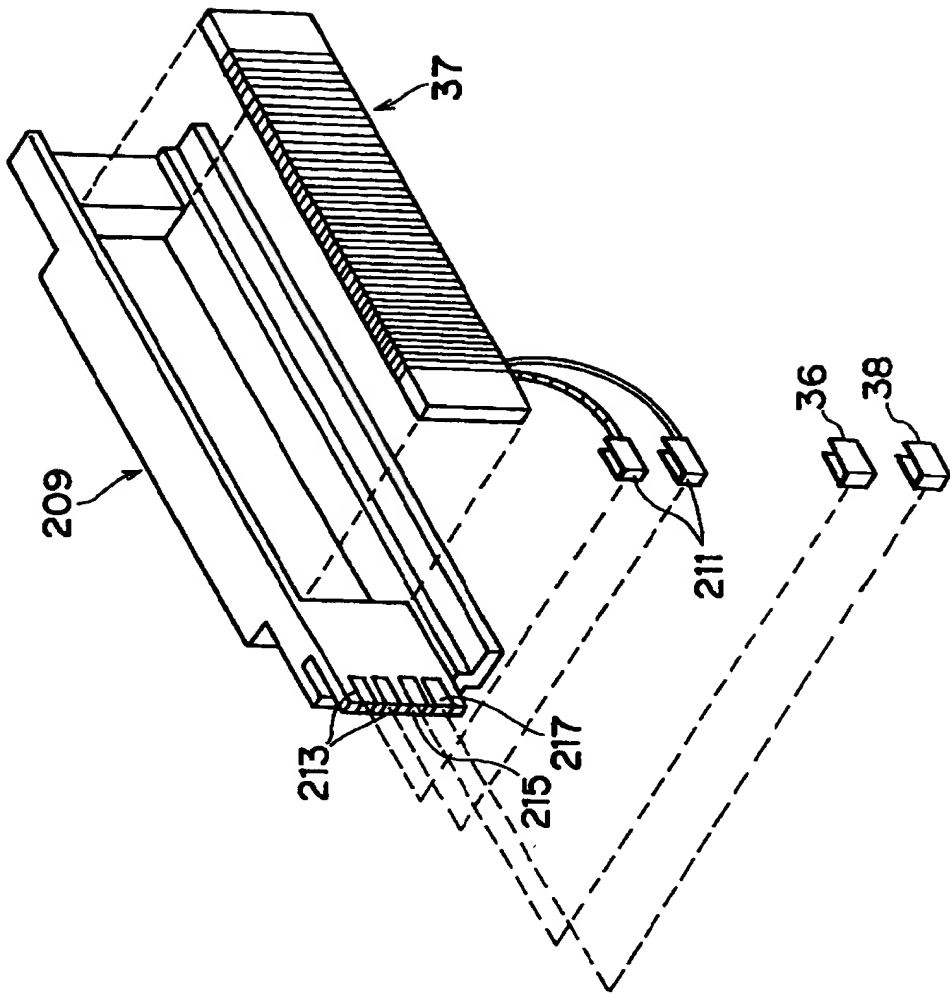
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 セキュリティ機能付きコンピュータのセキュリティ装置が不正に取り外された場合にコンピュータへのアクセスを禁止する。

【解決手段】 コンピュータの電源投入で、POSTプログラムが実行され、セキュリティ機能を有効にする設定で、RFIDチップ33は、Removal Detect Enableをハイレベルにしアナログスイッチ67の制御側及びNAND素子63の一方の入力側に出力する。RFアンテナ37が着脱されることにより第1短絡素子36が離間され端子71と端子73が遮断し、素子63のハイレベル信号でキーボード入力禁止のINTR信号が出力されコンピュータのアクセスを禁止する。電源オフでRFアンテナ着脱のときアナログスイッチ67を遮断し、リチウムバッテリーから供給のCMOSメモリ50への電力が遮断され、コンピュータへのアクセスを禁止することができる。

【選択図】 図2

認定・付加情報

特許出願の番号	平成11年 特許願 第205346号
受付番号	59900695070
書類名	特許願
担当官	鈴木 夏生 6890
作成日	平成11年 9月 8日

<認定情報・付加情報>

【特許出願人】

【識別番号】	390009531
【住所又は居所】	アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)
【氏名又は名称】	インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】	100086243
【住所又は居所】	神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	坂口 博

【代理人】

【識別番号】	100091568
【住所又は居所】	神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	市位 嘉宏

【復代理人】

【識別番号】	100079049
【住所又は居所】	東京都新宿区新宿4丁目3番17号 HK新宿ビル7階 太陽国際特許事務所
【氏名又は名称】	中島 淳

【選任した復代理人】

【識別番号】	100084995
【住所又は居所】	東京都新宿区新宿4丁目3番17号 HK新宿ビル7階 太陽国際特許事務所
【氏名又は名称】	加藤 和詳

【選任した復代理人】

【識別番号】	100085279
--------	-----------

次頁有

認定・付加情報（続き）

【住所又は居所】	東京都新宿区新宿四丁目3番17号	HK新宿ビル7階	太陽国際特許事務所
【氏名又は名称】	西元	勝一	
【選任した復代理人】			
【識別番号】	100099025		
【住所又は居所】	東京都新宿区新宿4丁目3番17号	HK新宿ビル7階	太陽国際特許事務所
【氏名又は名称】	福田	浩志	

出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 1990年10月24日

[変更理由] 新規登録

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレイション